# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/496,065 | 02/01/2000 | N. Asokan | SZ998-041 | 5668 |

| 7590 | 04/21/2004 |
|---|---|

Anne Vachon Dougherty Esq
IBM Corp
3173 Cedar Rd
Yorktown Heights, NY 10598

| EXAMINER |
|---|
| SIMITOSKI, MICHAEL J |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | 6 |

DATE MAILED: 04/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *09 February 2004*.
2a)☐ This action is **FINAL**.      2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-31* is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-31* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☒ All   b)☐ Some * c)☐ None of:
      1.☒ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
         application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

**Attachment(s)**
1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

## DETAILED ACTION

1.      Claims 1-31 are pending.

### *Response to Arguments*

2.      In light of applicant's amendments to the specification on (paper #5), the objections to the specification set forth in the previous office action (paper #4) are withdrawn.

3.      Applicant's arguments filed 2/11/04 have been fully considered but they are not persuasive. The rejections of claims 1, 3-5, 12-22 & 25-26 are maintained.

Regarding applicant's arguments concerning claim 1, applicant is directed to Fig. 3 of the Merritt reference where Merritt further discloses a storage component/card for storing predetermined authentication information/account info (Fig. 3) communicatable to the terminal for said terminal to create an authenticity output message (Fig. 3).

Regarding applicant's arguments concerning claim 3, Merritt discloses a device (processor and presentation module, Fig. 1) with a messaging component/presentation module and comparison component/comparator (Fig. 1). Merritt further discloses requesting user authentication information/PIN and verifying the authentication information/PIN with predefined values (see col. 1, lines 31-46).

Regarding applicant's arguments concerning claim 5 and the Giltner reference, the claimed invention (as stated by applicant, paper #5, page 29) "provides for storage of values in a lookup table". Giltner teaches that reducing the amount of data to be transmitted will reduce transmission time (see col. 1, lines 44-48). Giltner further teaches that by transmitting

addressing codes to a stored library, rather than transmitting the data in the library that the codes represent, can significantly reduce the data to be transmitted because the address code is much smaller than the data it represents (see col. 3, lines 14-32). As one having ordinary skill in the art knows, a lookup table is a structure used to associate one element/attribute to another. All data accessed via a memory is accessed by an address. Giltner simply teaches that in the context of data transmission, it is more efficient in time and storage requirements to transmit an index/addressing codes that are associated with a data of larger size than to transmit the data itself. By this teaching, it would have been obvious to transmit a value associated with an authenticity output message, such as is done in a lookup table, rather than the message itself.

Regarding applicant's arguments to claim 12, Merritt discloses a server/host authenticating a terminal/ATM (Fig. 3, #315), establishing a first authenticated trusted connection upon success of said authenticating (Fig. 3, #315) which also establishes a second trusted connection between the user/device and the server. Merritt further discloses the server authenticating it to the device/user by providing a terminal authenticity message/PSP sent to the terminal to be displayed to the user (second trusted connection) (Fig. 3, #380). Merritt lacks sending the authenticity to the device. The Manduley reference teaches that smart cards are useful in secure transactions, particularly as an electronic purse (as would be used at an ATM) (col. 1, lines 11-29). Manduley also teaches that exchanging messages between a user and a smart card is useful to make sure the correct user is using the smart card (col. 2, lines 7-23 & col. 1, lines 41-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send the authenticity output message to the smart card. Therefore, the rejection is maintained.

Regarding applicant's arguments to claim 25, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., applicant states that Daggar does not teach a devices having its own authentication component) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claim recites the limitation that the device is to be authenticated to the server. Daggar teaches the well-known concept in the art that device authentication is crucial in secure transactions.

Regarding applicant's arguments against the Manduley patent, specifically that Manduley doesn't teach sending terminal authentication directly from a server to the device, applicant is directed to applicant's specification on pages (10, 12 & 17) where the second connection is "tunneled" through the first connection. Tunneling through an intermediary is not a direct connection. Applicant is invited to bring to the examiner's attention where in the specification a direct connection not involving the terminal is made between the server and the device. Moreover, Merritt discloses sending a terminal authenticity message to a user through the terminal, which only happens when the terminal is authenticated. Manduley teaches that using smart cards is well known in secure transactions. Manduley also teaches that it is well known as beneficial for a smart card to contain a display for interacting with the user to avoid blind use of the device by anyone. While the information from the user's card is given to the terminal before authentication, the claims do not state that the terminal must be trusted *before* the user accesses the terminal.

Regarding applicant's arguments against the Lessin reference, once again, the claims do

not recite a limitation where a user is only inclined to enter personal information, such as a pin to

the terminal after the authentication message has arrived.

4.      Applicant's arguments, see paper #5 pages 24-25, filed 2/11/04, with respect to the

enablement rejections claims 23 & 24 have been fully considered and are persuasive. The

rejection of claims 23 & 24 has been withdrawn. However, upon further consideration, a new

ground(s) of rejection is made in view of Applied Cryptography, Second Edition by Schneier

(see below).

5.      Applicant's arguments with respect to claims 2, 6-8 & 27-31 have been considered but are

moot in view of the new ground(s) of rejection.

## Claim Rejections - 35 USC § 112

6.      The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making
> and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it
> pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode
> contemplated by the inventor of carrying out his invention.

7.      Claim 9 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the

written description requirement. The claim(s) contains subject matter which was not described

in the specification in such a way as to reasonably convey to one skilled in the relevant art that

the inventor(s), at the time the application was filed, had possession of the claimed invention.

The written description (pages 10, 12, 17) discloses that the authenticity output message is sent

using the second connection which is "tunneled" through the first connection and is therefore not

sent directly to the device. Claims 10-11 are rejected based on their dependence upon claim 9.

8.       The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9.       Claim 29 recites the limitation "wherein generating" in lines 5-6. There is insufficient

antecedent basis for this limitation in the claim. Because it is unclear as to which step "wherein

generating ..." is referring, this limitation will not be addressed.

## *Claim Rejections - 35 USC § 102*

10.     The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11.     Claims 1, 3, 4, 6, 7, 9-11 & 31 are rejected under 35 U.S.C. 102(b) as being anticipated

by U.S. Patent 5,475,756 to Merritt.

Regarding claim 1, Merritt discloses a terminal that can communicate with a personal

device/card (see Fig. 1). The terminal is connected to a server/host (see Fig. 1) and the

terminal/ATM authenticates itself with the server/host (see Fig. 3, element 315). Authentication

information is contained on the card (see col. 3, lines 64-67 and col. 4, lines 1-11) to be read by

the terminal/ATM (see Fig. 3). Merritt discloses a terminal displaying an authenticity output

message/PSP in response to authentication (see Fig. 5 and col. 3, lines 20-48). Merritt further

discloses a storage component/card for storing predetermined authentication information/account

info (Fig. 3) communicatable to the terminal for said terminal to create an authenticity output

message (Fig. 3).

Regarding claim 3, Merritt discloses requesting user authentication information/PIN and

verifying the authentication information/PIN with predefined values (see col. 1, lines 31-46).

Regarding claim 4, Merritt discloses a message/PSP taking many forms, such as a still

image, a sequence of images, a video or an audio clip (see col. 4, lines 16-23).

Regarding claim 6, Merritt discloses a terminal with a device input component/card

reader (see Fig. 1, element 14), communication component (see Fig. 1, element 9), a message

creation component/presentation module for dynamically creating at least one authenticity output

message/PSP upon authentication by the server (Fig. 3) and at least one message output

component for outputting the authenticity message/PSP to the user (Fig. 3). Note that

'dynamically' is defined as "Characterized by continuous activity" (American Heritage College

Dictionary).

Regarding claim 7, Merritt discloses a user interface component/keyboard (see Fig. 1,

element 21).

Regarding claims 9 and 11, Merritt discloses a server/host (Fig. 1, element 2), a

communications component (see Fig. 1, element 9), a receiver means (see Fig. 3, elements 310

and 360), an authenticity component to verify the terminal's authenticity (see Fig. 1, elements 4

and 8, Fig. 3, element 315 and col. 2, lines 10-14) and a message generation component (see Fig.

1, element 3) and a storage location (see Fig. 1, element 3) for storing a user-specific authenticity

output message/PSP (see col. 4, lines 11-20).

Regarding claim 10, Merritt discloses the host and the terminal negotiating a session key

(see col. 6, lines 54-62).

Regarding claim 31, Merritt discloses receiving user-specific authentication

information/account information from a device/card for use in creating said authenticity output

message/PSP (Fig. 3).

12. Claim 27 is rejected under 35 U.S.C. 102(b) as being anticipated by "Trusting Mobile

User Devices and Security Modules" by Pfitzmann et al. (Pfitzmann). Pfitzmann discloses

requesting a terminal/mobile user device including security module to obtain

authentication/identification by a server/second security module (page 64, Fig. 3, #1), receiving a

terminal authenticity message/DIN from said server/second security module (page 64, Fig. 3, #2)

and causing an authenticity output message to be displayed/shown to said user (page 64, Fig. 3,

#3).

### Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

14.     Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Merritt in view of

Pfitzmann. Merritt discloses a system, as described above, but lacks authenticating the card to

the terminal. However, Konigs teaches that to achieve a secure transaction, a mutual

authentication must occur between a Card Adapter Device and a smart card (page 43 & Fig. 2).

The smart card contains an authentication component (Fig. 2). Therefore, it would have been

obvious to one having ordinary skill in the art at the time the invention was made to include an

authentication component in Merritt's card. One of ordinary skill in the art would have been

motivated to perform such a modification to complete secure transactions, as taught by Konigs

(page 43 & Fig. 2). As modified, Merritt lacks the limitation that the device authenticates itself

to the terminal upon receipt of the terminal authentication information from said server.

However, Pfitzmann teaches that to prevent fake device attacks, a user can rely on cryptographic

protocols to identify devices (page, 64 §*Fake Device Attacks*). Pfitzmann teaches that a user

only authenticates himself to a terminal/mobile security device upon receiving authentication

information/DIN from a server/second security module (page 64 Fig. 3 & §*Fake Device Attacks*).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the

invention was made to use Pfitzmann's authentication scheme to authenticate a personal device

to a terminal upon receipt of terminal authentication information from the server. One of

ordinary skill in the art would have been motivated to perform such a modification to prevent

fake device attacks, as taught by Pfitzmann (page 64 Fig. 3 & §*Fake Device Attacks*).


15.     Claims 5 & 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merritt, as

applied to claim 1 above, in view of U.S. Patent 4,386,416 to Giltner et al. (Giltner). Merritt

discloses an authentication system, as described above, but lacks storing a lookup table.

However, Giltner teaches that reducing the amount of data to be transmitted will reduce

transmission time (see col. 1, lines 44-48). Giltner further teaches that by transmitting

addressing codes to a stored library, rather than transmitting the data in the library that the codes

represent, can significantly reduce the data to be transmitted because the address code is much

smaller than the data it represents (see col. 3, lines 14-32). Therefore, it would have been

obvious to one having ordinary skill in the art at the time the invention was made to store the

authenticity output message in a lookup table in the terminal to reduce transmission time. One of

ordinary skill in the art would have been motivated to perform such a modification to reduce the

amount of data transmitted and hence reduce transmission time, as taught by Giltner.

16.     Claims 12-19, 21, 22 & 26 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Merritt in view of U.S. Patent 5,737,423 to Manduley.

Regarding claims 12 & 21, Merritt discloses a server/host authenticating a terminal/ATM

(Fig. 3, #315), establishing a first authenticated trusted connection upon success of said

authenticating (Fig. 3, #315) which also establishes a second trusted connection between the

user/device and the server. Merritt further discloses the server authenticating it to the

device/user by providing a terminal authenticity message/PSP sent to the terminal to be

displayed to the user (second trusted connection) (Fig. 3, #380). Merritt lacks sending the

authenticity to the device. The Manduley reference teaches that smart cards are useful in secure

transactions, particularly as an electronic purse (as would be used at an ATM) (col. 1, lines 11-

29). Manduley also teaches that exchanging messages between a user and a smart card is useful

to make sure the correct user is using the smart card (col. 2, lines 7-23 & col. 1, lines 41-56).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the

invention was made to send the authenticity output message to the smart card. One of ordinary

skill in the art would have been motivated to perform such a modification because smart cards

are used in secure transactions and because the legitimate user of the card will be reading the

messages, as taught by Manduley (col. 2, lines 7-23 & col. 1, lines 41-56).

Regarding claim 13, Merritt discloses communicating a message to a user (see Fig. 5,

element 515).

Regarding claims 14, 17 & 19 Merritt discloses a smart card system, as described above,

but lacks displaying messages on the card. Manduley teaches that by exchanging a set of

messages between a user and a smart card (see col. 2, lines 7-23), one can assure that the user is

actually in possession of the card (see col. 1, lines 41-56). Therefore, it would have been

obvious to one having ordinary skill in the art at the time the invention was made to incorporate a

visual display in Merritt's smart card for the purposes of exchanging messages between the user

and the card. One of ordinary skill in the art would have been motivated to perform such a

modification to ensure that the person responding to a message is actually in possession of the

card, as taught by Manduley.

Regarding claim 15, Merritt discloses a terminal displaying a message (see col. 3, lines

40-45).

Regarding claim 16, Merritt discloses accessing a database/lookup table that stores user-

specific messages/PSPs (see col. 7, lines 1-10).

Regarding claim 18, Merritt discloses authentication information contained on the card (see col. 3, lines 64-67 and col. 4, lines 1-11) to be read by the terminal/ATM (see Fig. 3). Merritt discloses a terminal displaying an authenticity output message/PSP in response to authentication (see Fig. 5 and col. 3, lines 20-48).

Regarding claim 22, Merritt discloses a message/PSP taking many forms, such as a still image, a sequence of images, a video or an audio clip (see col. 4, lines 16-23).

Regarding claim 26, Merritt discloses authenticating a user (see Fig. 3, element 390).


17.     Claims 23 & 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merritt in view of Manduley, as applied to claim 21 above, in further view of Schneier. Merritt, as modified above, lacks partially outputting a message. However, Schneier teaches that SKEY is a known authentication protocol (as the PSP is used to authenticate the server/host). In SKEY, each entity has a list of numbers (message). One of the numbers is outputted to be recognized by the other entity (partial message) (page 53). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the SKEY protocol for authentication using a message/PSP. One of ordinary skill in the art would have been motivated to perform such a modification because an eavesdropper gains no information about the message in that each output of the message is used only once (page 53).


18.     Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Merritt in view of Manduley, as applied to claim 12 above, in further view of U.S. Patent 4,868,376 to Lessin et al. (Lessin). Merritt discloses a smart card system, as described above, but lacks the card requesting

the user authenticate himself. Lessin teaches that by requiring the user enter a PIN, a card can

prevent unauthorized access to data (see col. 4, lines 7-11 and col. 8, lines 27-41). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was

made to modify Merritt's smart card system to request the user authenticate himself to prevent

unauthorized access. One of ordinary skill in the art would have been motivated to perform such

a modification to prevent unauthorized access to data on the card, as taught by Lessin.

19.     Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Merritt in view of

Manduley, as applied to claim 12 above, in view of U.S. Patent 5,748,737 to Daggar. Merritt

discloses a smart card system, as described above, but lacks authenticating the card to the server.

Daggar teaches that establishing card authenticity is needed to make sure data from a card is

genuine and to prevent indiscriminate card reproduction (see col. 7, lines 13-19). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was

made to have Merritt's server authenticate the card to ensure data integrity. One of ordinary skill

in the art would have been motivated to perform such a modification to ensure the data from the

card is genuine and to prevent indiscriminate card reproduction, as taught by Daggar.

20.     Claims 28 & 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Pfitzmann, as applied to claim 27 above, in view of Konigs in further view of Manduley.

        Regarding claim 28, Pfitzmann discloses a system, as described above, but lacks the

authenticity output message displayed by a user device. However, Konigs teaches that smart

cards are useful in authentication because of their key capacity and ability to perform

cryptography (page 42 ¶1). Konigs teaches a system where the user identifies himself to the

smart card and the smart card identifies itself to the terminal (pages 42-43). Therefore, it would

have been obvious to one having ordinary skill in the art at the time the invention was made to

authenticate the user to the security mobile device using a smart card. One of ordinary skill in

the art would have been motivated to perform such a modification to authenticate a user to a

terminal through the use of long cryptographic keys, as taught by Konigs (pages 42-43). As

modified, Pfitzmann lacks providing a terminal authenticity message to the device. However,

Manduley teaches that by exchanging a set of messages between a user and a smart card (col. 2,

lines 7-23), one can assure that the user is actually in possession of the card because the

authenticated user is the only person able to read the messages (col. 1, lines 41-56). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was

made to provide the smart card of Konigs system with an authenticity message/DIN so the

server/second security module is ensured the user is in possession of the smart card and receiving

the messages. One of ordinary skill in the art would have been motivated to perform such a

modification to guarantee the server that the person receiving a message is the person actually in

possession of the card, as taught by Manduley (col. 1, lines 41-56 & col. 2, lines 7-23).

Regarding claim 30, Pfitzmann discloses authenticating a terminal (page 64, Fig. 3, #1).

It is inherent that the terminal must receive input to being the process and establish the correct

DIN. Pfitzmann discloses generating a terminal authenticity message for delivery to the user

(page 64, Fig. 3, # 2-3), but not to a user device. However, Konigs teaches that smart cards are

useful in authentication because of their key capacity and ability to perform cryptography (page

42 ¶1). Konigs teaches a system where the user identifies himself to the smart card and the smart

card identifies itself to the terminal (pages 42-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate the user to the security mobile device using a smart card/personal device. One of ordinary skill in the art would have been motivated to perform such a modification to authenticate a user to a terminal through the use of long cryptographic keys, as taught by Konigs (pages 42-43). As modified, Pfitzmann lacks providing the terminal authenticity message to the device. However, Manduley teaches that by exchanging a set of messages between a user and a smart card (col. 2, lines 7-23), one can assure that the user is actually in possession of the card because the authenticated user is the only person able to read the messages (col. 1, lines 41-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide the smart card of Konigs system with an authenticity message/DIN so the server/second security module is ensured the user is in possession of the smart card and receiving the messages. One of ordinary skill in the art would have been motivated to perform such a modification to guarantee the server that the person receiving a message is the person actually in possession of the card, as taught by Manduley (col. 1, lines 41-56 & col. 2, lines 7-23).

21.    Claim 29, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over Pfitzmann, as applied to claim 27 above, in view of Konigs. Pfitzmann further discloses said authenticity output message/DIN being created and displayed by the terminal/mobile security device with secure module (page 64, Fig. 3), but lacks a user device providing user-specific authentication information to said terminal. However, Konigs teaches that smart cards are useful in authentication because of their key capacity and ability to perform cryptography

(page 42 ¶1). Konigs teaches a system where the user identifies himself to the smart card and the

smart card identifies itself to the terminal (pages 42-43). Therefore, it would have been obvious

to one having ordinary skill in the art at the time the invention was made to authenticate the user

to the security mobile/terminal device using a smart card, where the user device/smart card

provides user-specific authentication information (keys and encrypted data according to one of

the many authentication protocols disclosed by Konigs) to the terminal/mobile security device.

One of ordinary skill in the art would have been motivated to perform such a modification to

authenticate a user to a terminal through the use of long cryptographic keys, as taught by Konigs

(pages 42-43).


## *Conclusion*

22.     Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The

examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached on (703)308-4789.

> **Any response to this action should be mailed to:**
> Commissioner of Patents and Trademarks
> Washington, DC 20231
> **Or faxed to:**
> (703)746-7239 (for formal communications intended for entry)
> **Or:**
> (703)746-7240 (for informal or draft communications, please label "PROPOSED"
> or "DRAFT")
> Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive,
> Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
April 12, 2004

NORMAN M. WRIGHT
PRIMARY EXAMINER